REMARKS

Claims 1-65 remain in the application. Claims 1-65 were rejected. Applicant respectfully thanks the examiner for his time in the personal interview of 15 March 2004. In the interview, the Klayh reference was discussed.

Double Patenting

Claims (1, 12, 13, 32-24), (2-11, 14-20, 28 and 35-39), (21-31 and 40), (50-54) and (55-65) are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-45 of U.S. patent No. 6,394,907 to Rowe. A terminal disclaimer is provided with the response and the rejections are believed overcome thereby.

Rejections under 35 U.S.C. § 102(e)

Claims 1, 9-13 and 32-34 are rejected under 35 U.S.C. 102(e) as being anticipated by Klayh, U.S. 2003/0050831 A1. The rejection is respectfully traversed.

The present invention, as recited in the pending claims, describes a cashless instrument transaction clearinghouse where "the cashless instrument transaction clearinghouse at least (i) receives cashless instrument validation requests from a first property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property and (ii) sends information to a second gaming property requesting the second property to approve or reject the cashless instrument validation request." Applicant believes this limitation is not described by the Klayh reference. The reasons for this assertion are enumerated as follows.

Klayh teaches establishing an individual account for a player and then issuing the player and ID card with a PIN number that allows the player access the account (Paragraphs 47-49). The player can add credits to their account, which is stored in a database on a remote server. The player can gain access to their account at a number of locations by providing their ID card and entering the correct PIN number (Paragraphs 62-64). For instance, the player may wish to gain access to credits stored on their account. If an account is not located on a first server, the first server attempts to contact remote servers to see if the remote servers have a record of the player's account and to determine for instance if there credits in the account if the player wishes to use them (Paragraphs 71-72).

To allow access to an account using an ID card as described in Klayh, a PIN is matched to an account number stored on the card. As is known in the art, most cards use the "IBM Pin Derivation Method". A 16 digit account number is taken as a hexadecimal string. This is then converted to a 64 bit block, which is encrypted using a special "PIN Derivation Key". The

resulting ciphertext is converted back into hexadecimal, and all but the first four characters are discarded. Any occurrences of the letters A thru F are converted to 0 thru 5 using a simple substitution table. The result is a PIN number that is associated with the 16 digit account number. To change the PIN number, an offset to the original PIN, which marks the difference between old and new is added. These offsets are not securely stored, as without the root PIN, they are useless. Thus, when a user enters the correct PIN, it is assumed they should be granted access to the account number stored on the card. Typically, these cards do not store any information in regards to the value of anything that can be obtained with card only the account number. The value information is stored in the remote account.

In the present invention, a cashless instrument is generated. The cashless instrument stores information that describes the cashless instrument (e.g., but not limited to a serial number and a location where it was issued) and can store/record information that describes something of value that may be obtained with the card (e.g., but not limited to cash, credits, promotional credits, etc.). When the cashless instrument is generated, a portion of the information stored on the cashless instrument is stored on another device. Unlike Klayh, the cashless instruments of the present invention do not have to be associated with a player and/or an account associated with the player. Further, unlike Klayh, the cashless instruments are typically used to store/record a value associated with instrument. As one example, for printed cashless instruments, the value of the cashless instrument is printed on the ticket. This allows the player to confirm what the cashless instrument is worth.

When a cashless instrument is validated, information stored on the cashless instrument is compared with information stored at another location. The information stored at the other location may include but is not limited to information that allows the cashless instrument to be identified, where it was generated, its value and whether it has been previously redeemed. The information describing whether the cashless instrument has been previously redeemed is for preventing someone from generating a duplicate of the cashless instrument and then attempting to redeem it multiple times.

In the present invention, a cashless instrument may be generated at a first property. At the first property, information regarding the cashless instrument used for validation purposes is stored. Then, an attempt can be made to use the cashless instrument at a second property using the cashless instrument transaction clearinghouse. As described in the pending claims, "the cashless instrument transaction clearinghouse at least (i) receives cashless instrument validation requests from a first property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property and (ii) sends information to a second gaming property requesting the second property to approve or reject the cashless instrument validation request." The information sent to the second gaming property may be used by the second gaming property to determine if the cashless instrument is valid, e.g., but not limited to,

whether the second property has a record of the cashless instrument and whether the cashless instrument has been previously redeemed.

In Klayh, there is no attempt to validate the ID card. If a PIN number is entered that corresponds to the account stored on the card, access is granted to the account whether it is a valid card or not. This is why, as it well know in the banking industry, it is possible to create a fraudulent bank card and gain access to a user's bank account if one is able to steal the account number and the associated PIN number. As described above, Klayh teaches ID cards that are used to access a user's account. Further, a value of something that can be obtained with the card is not stored or recorded on the card. Therefore, since the ID card in Klayh is not validated and the card is strictly used to gain access to a player's account without storing or recording a value of something that can be obtained with the card, for at least these reasons, Klayh can't be said to anticipate or render obvious the invention 1, 9-13 and 32-34 and the rejection is believed overcome thereby.

Rejections under 35 U.S.C. § 103

Claims 2-8, 14-20, 28 and 35-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, B, "Applied Cryptography." **(Note: Applicant is assuming from Examiner's response that this rejection is Klayh in view of Schneier.)**

Examiner relies on Schneier to teach encryption methods. Klayh, for the reasons cited above, does not anticipate or render obvious the present invention. Schneier does not overcome the deficiencies cited in Klayh. Therefore, for at least these reasons, the combination of Klayh and Schneier can't be said to render obvious the present invention and the rejection of claim 2-18, 14-20, 28 and 35-39 is believed overcome thereby.

Claims 21-27, 29-31 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Klayh in view of Schneier in further view of Fox (6, 560,581).

Examiner relies on Schneier and Fox to teach encryption method. Klayh, for the reasons cited above, does not anticipate or render obvious the present invention. Schneier and Fox do not overcome the deficiencies cited in Klayh. Therefore, for at least these reasons, the combination of Klayh, Schneier and Fox can't be said to render obvious the present invention and the rejection of claim 21-27, 29-31 and 40 is believed overcome thereby.

Claims 50-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Klayh in view of Schneier in further view of Gennaro (5, 937, 066).

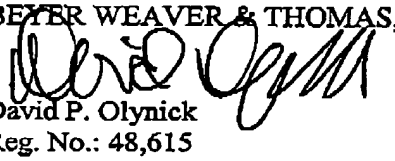
Examiner relies on Schneier and Gennaro to teach encryption method. Klayh, for the reasons cited above, does not anticipate or render obvious the present invention. Schneier and Gennaro do not overcome the deficiencies cited in Klayh. Therefore, for at least these reasons, the combination of Klayh, Schneier and Gennaro can't be said to render obvious the present invention and the rejection of claim 50-54 is believed overcome thereby.

Claims 55-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Klayh in view of Schneier and Fox in further view of Gennaro (5, 937, 066).

Examiner relies on Schneier, Gennaro and Fox to teach encryption method. Klayh, for the reasons cited above, does not anticipate or render obvious the present invention. Schneier, Gennaro and Fox do not overcome the deficiencies cited in Klayh. Therefore, for at least these reasons, the combination of Klayh, Schneier, Fox and Gennaro can't be said to render obvious the present invention and the rejection of claim 55-65 is believed overcome thereby.

Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP



David P. Olynick
Reg. No.: 48,615

P.O. Box 778
Berkeley, CA 94704-0778
510-843-6200